UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America,

Plaintiff,

v.

John Frederick Krisnik,

Defendant.

Crim. No. 18-32 (JNE/BRT)

REPORT AND RECOMMENDATION

Katharine T. Buzicky, Esq., Assistant United States Attorney, counsel for Plaintiff.

Patrick L. Cotter, Esq., Sieben & Cotter, PLLC, counsel for Defendant.

On February 14, 2018, Defendant was indicted by a grand jury for receipt of child pornography, access with intent to view child pornography, and possession of child pornography. (Doc. No. 1, Indictment.) Defendant John Frederick Krisnik now moves to suppress evidence obtained pursuant to a warrant that authorized the search of Defendant's residence for evidence of child pornography offenses. (Doc. No. 22, Def.'s Mot.)

The Court held a hearing on the motion to suppress on July 9, 2018. (Doc. No. 28.) At the hearing, the Government introduced the warrant application and an inventory of items seized as exhibits. (Doc. No. 29, Gov't Exs. 1, 2.) Defendant requested a four-corner review of the warrant and additional briefing on the motion. (Doc. No. 28.) The motion was taken under advisement on August 6, 2018. (*See id.*)

For the reasons set forth below, this Court recommends that Defendant's motion to suppress be denied.

I. Background

The search warrant affidavit at issue was prepared by FBI Special Agent Robert J.E. Blackmore. (Gov't Exs. 1, 2.) SA Blackmore's investigation concerned violations of 18 U.S.C. § 2252(a)(4)(B), which prohibits knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. (Gov't Ex. 1 at 3.)[1] In the affidavit, SA Blackmore averred that he had "probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252(a)(4)(B) (access with intent to view child pornography)" were located in the subject premises. (*Id.* at 1.)

SA Blackmore's affidavit contained information regarding a nationwide investigation of users of a website referred to as "Website A,"[2] and the technology that

---

[1] At the time of the search, SA Blackmore had been an FBI agent for more than fourteen years and was a member of the Child Exploitation Task Force. (Gov't Ex. 1 at 1.) His work involves investigating child sexual exploitation offenses committed using computers, computer networks, and the Internet. (*Id.*)

[2] SA Blackmore averred that the "actual name of 'Website A' is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the

(Footnote Continued on Next Page)

allowed the FBI to identify them. (*Id.* at 13–26.) Website A existed on the Tor Network,[3] which "facilitate[s] anonymous communication over the Internet." (*Id.* at 14.) Tor prevents third parties from learning "what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the [Tor] Network routes communication through other computers, traditional IP identification techniques are not viable." (*Id.* at 14–15.)

According to SA Blackmore, it would be "extremely unlikely that any user could have simply stumbled upon 'Website A' without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography." (*Id.* at 16.) To view the contents of Website A, a user had to (1) install software, (2) obtain the (non-searchable) web address of Website A, (3) become a member of the site, and (4) log in to the site. (*Id.* at 15–16, 18–19.)

The FBI seized a copy of Website A from a server in North Carolina on February 20, 2015. (*Id.* at 17.) The FBI allowed Website A to operate from a server in Virginia until March 4, 2015. (*Id.* at 17.) During that time, the FBI obtained a warrant to

---

(Footnote Continued From Previous Page)
fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence." (Gov't Ex. 1 at 13 n.1.) In its brief, the Government states that Website A's true name is now public, but does not use the publicly-known name. (Doc. No. 31, Gov't's Br. 2 n.2.) This Court will use the term "Website A" for consistency and to avoid confusion.

[3] The search warrant affidavit uses the term "The Network," but the Government's brief identifies the network by name. (Gov't's Ex. 1 at 14; Gov't's Br. 2.)

deploy the Network Investigative Technique ("NIT") and obtain information about Website A's users. (*Id.* at 25.) The NIT would capture, among other things, the user's actual IP address and the computer's operating system name, host name, and Media Access Control ("MAC")[4] address. (*Id.* at 25–26.) An IP address is a "unique number used by a computer to access the Internet." (*Id.* at 10.) After obtaining the IP address, the FBI could use publicly-available websites to look up the owner of the IP address, and then serve a subpoena or other legal process to find the individual user assigned to that address. (*Id.* at 29.)

According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, a user with the user name "baddaddy" spent 112 hours and 52 minutes on Website A between November 26, 2014, and February 24, 2015. (*Id.* at 26–27.) "Baddaddy" made approximately fifteen postings during that timeframe. (*Id.* at 27.) For example, on January 29, 2015, another user made a post entitled "My collection vids," which included a series of preview images of child pornography and child erotica. (*Id.* at 27.) Several users posted comments, including baddaddy, who replied on January 30, "Wow great collection! I can't wait to see them all. BadDaddy." (*Id.*) Similarly, on or about January 17, 2015, a user made a post entitled

[4] A MAC address is typically assigned to a computer's network adapter by the manufacturer. (Gov't's Ex. 1 at 10–11.) "A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC can allow law enforcement to identify whether communications sent or received are associated with the same adapter." (*Id.* at 11.)

"[OC] Chubby Ester 15 yo." (*Id.* at 27–28.) On or about February 22, 2015, baddaddy replied, "I LOVE chubby teens! Thank you! BadDaddy." (*Id.* at 28.)

The FBI also determined that on February 22, 2015, baddaddy accessed a post entitled "PedoDogs PedoWomen Picture Pack" from IP address 71.82.138.217. (*Id.* at 28–29.) Among other things, this post contained hyperlinks to external websites containing preview images, also known as contact sheets, as well as hyperlinks to the full files and a password to open the files. (*Id.* at 29.) The contact sheet contained over 200 smaller images, many of which contained child pornography and child erotica depicting prepubescent and early pubescent males and females. (*Id.*) Using publicly available websites, FBI Special Agents were able to determine that the above IP address was operated by Internet Service Provider ("ISP") Charter Communications. (*Id.*) In March 2015, an administrative subpoena was served upon Charter Communications requesting information related to the user assigned to the above IP address. (*Id.*) In response, Charter advised that for the requested date and time, the IP address was accessed by the account subscribed in Defendant's name at Defendant's residence, with an installation date of June 7, 2013. (*Id.*) Service was current as of March 11, 2015. (*Id.*)

After linking Defendant to the IP address captured by the NIT, SA Blackmore next linked Defendant to the residence through Postal Service queries, physical surveillance of the residence, motor vehicle records, Accurint databases, and publicly-available Facebook posts. (*Id.* at 29–31.) Surveillance showed two of Defendant's vehicles parked in the driveway of the home. (*Id.* at 30.) In addition, the host name of the computer

associated with the IP address, John8370, mirrored Defendant's name and street number. (*Id.* at 31.)

Finally, SA Blackmore's affidavit explained some common characteristics of individuals who commit the offense of access with intent to view child pornography, such as collecting and storing child pornography images in a secure environment, like their home. (*Id.* at 31–34.) The affidavit then noted that some of Defendant's actions comported with these common characteristics. (*Id.* at 34–35.) The affidavit also explained characteristics of computers that make them "ideal repositor[ies] for child pornography." (*Id.* at 37.) Data storage on a computer can be "intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites," or it can be unintentional, such that "traces of the path of an electronic communication may be automatically stored in many places" and the way a "user's Internet activities generally leave traces or 'footprints' in the web cache and history files of the browser used." (*Id.* at 38–39.) As stated in the affidavit, computer forensic professionals "can recover even hidden, erased, compressed, password-protected, or encrypted files." (*Id.* at 40.)

The search warrant issued on July 27, 2015, and was executed on July 29, 2015. (*See* Exs. 1, 2.) The warrant authorized officers to search Defendant's residence for evidence of violations of 18 U.S.C. § 2252(b)(4)(B), Access with Intent to View Child Pornography. (*See* Ex. 1.) Officers seized, among other items, several laptop computers, a desktop computer, two external hard drives, a flip phone, DVDs, CDs, and video tapes. (Gov't Ex. 2 at 11.)

II. Analysis

Defendant argues that SA Blackmore's affidavit did not provide probable cause for the warrant because there was an insufficient nexus between the items to be seized and his residence, and the facts supporting the search warrant were stale. (Doc. No. 23, Def.'s Mem. 1–11.) The Government asserts that there was probable cause to search Defendant's home because the FBI identified a particular computer connecting to Website A from Defendant's internet account. (Doc. No. 31, Gov't's Mem. 6.) Thus, according to the Government, there was a sufficient nexus between Defendant's residence and child pornography established by timely, recent information. (*Id.* at 6–13.) And even if not supported by probable cause, the Government argues that the officers acted in good faith reliance on the judge's decision to grant the warrant and authorize the search. (*Id.* at 13.)

A. The Search Warrant Was Supported by Probable Cause

"Whether probable cause to issue a search warrant has been established is determined by considering the totality of the circumstances." *United States v. Notman*, 831 F.3d 1084, 1088 (8th Cir. 2016). "If an affidavit in support of a search warrant sets forth sufficient facts to lead a prudent person to believe that there is a fair probability that contraband or evidence of a crime will be found in a particular place, probable cause to issue the warrant has been established." *Id.* "Probable cause does not require evidence sufficient to support a conviction, nor even evidence demonstrating that it is more likely than not that the suspect committed a crime." *United States v. Donnelly*, 475 F.3d 946, 954 (8th Cir. 2007). In determining whether probable cause exists, courts "apply a

common sense approach . . . considering all relevant circumstances." *United States v. Hager*, 710 F.3d 830, 836 (8th Cir. 2013). A reviewing court must "pay 'great deference' to the probable cause determinations of the issuing judge or magistrate, and limit [its] inquiry to discerning whether the issuing judge had a substantial basis for concluding that probable cause existed." *United States v. Butler*, 594 F.3d 955, 962 (8th Cir. 2010) (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). "When the [issuing judge] relied solely upon the supporting affidavit to issue the search warrant, only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause." *United States v. O'Dell*, 766 F.3d 870, 874 (8th Cir. 2014).

The facts of this case are similar to *United States v. Huyck*, which held that a warrant seeking evidence relating to access with intent to view child pornography was supported by probable cause. 849 F.3d 432, 438–40 (8th Cir. 2017). The facts alleged in the *Huyck* affidavit, like the affidavit in the instant case, related to access, and the warrant did not contain any evidence of downloading activity. *Id.* at 436. The defendant in *Huyck* argued that "briefly browsing a child pornography website is not sufficiently likely to result in evidence of child pornography possession four-and-one-half months later." *Id.* at 439. The court rejected this argument, reasoning that the defendant "did not simply and accidentally navigate to Pedoboard for a few meaningless minutes. Instead, the evidence shows he accessed Pedoboard after taking a number of intermediate steps that indicated

his knowledge that Pedoboard trafficked in child pornography." *Id.*[5] Similarly here, to view the contents of Website A, a user such as Defendant had to (1) install software, (2) obtain the (non-searchable) web address of Website A, (3) become a member of the site, and (4) log in to the site. *See id.* ("'Accessing PedoBook therefore required numerous affirmative steps by the user, making it extremely unlikely that a user would stumble upon it without knowing that its purpose was to advertise and distribute child pornography and understanding the content to be found there.'") (quoting *United States v. DeFoggi*, 839 F.3d 701, 707 (8th Cir. 2016)). Moreover, while the affidavit in *Huyck* documented only nine minutes of Pedoboard activity, SA Blackmore's affidavit documented 112 hours of Website A activity, along with fifteen separate postings on Website A. SA Blackmore also obtained a host name for Defendant's computer, an instrumentality of the offense, that correlated to Defendant's name and address. Therefore, the evidence in support of probable cause is even stronger than it was in *Huyck*.

Defendant argues that there is no nexus between his home and the items to be seized because the affidavit only states that he accessed or viewed child pornography, not that he downloaded or uploaded child pornography. (Def.'s Mem. 5–7.) The analysis does not differ, however, when the crime alleged in the search warrant affidavit is access

[5] The defendant in *Huyck* also argued that "there is a difference between someone who downloads child pornography and someone who browses through child pornography." 849 F.3d at 439. The court rejected this argument because the defendant did not "proffer any evidence demonstrating a difference in the habits of those browsing through child pornography and those downloading child pornography." *Id.*

with intent to view child pornography. *See Huyck*, 849 F.3d at 436, 438–40. Here, the FBI used subpoenas to link Defendant to the IP address captured by the NIT, and then linked Defendant to the residence through Postal Service information, physical surveillance of the residence, motor vehicle records, Accurint databases, Facebook, and the "John 8370" host name recorded by the NIT. (Gov't Ex. 1 at 29–31); *see United States v. Stults*, 575 F.3d 834, 844 (8th Cir. 2009) (affirming probable cause where search warrant affidavit showed IP address used to access child pornography sites was traced to defendant); *United States v. Tagg*, 886 F.3d 579, 590 (6th Cir. 2018) (finding sufficient nexus where "police linked the IP address he used to access Playpen to the residence listed on the warrant, and even observed him entering and exiting the premises"). The host name also identified the computer and its component parts, which are "instrumentalities of violations of 18 U.S.C. § 2252(a)(4)(B)." (Gov't Ex. 1 at 1.)

Finally, the warrant in *Huyck* sought "not just contraband—that is additional child pornography—but evidence related to [defendant's] prior . . . crimes of receiving child pornography and accessing with intent to view child pornography." 849 F.3d at 440. The "prior crime" referenced in *Huyck* was the nine minutes of Pedoboard activity that investigators linked to the defendant's IP address. *Id.* at 436. Similarly here, the warrant sought evidence relating to Defendant's prior crimes of accessing with intent to view child pornography by browsing and using Website A. The affidavit in this case, like the affidavit in *Huyck*, explained that "[d]igital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among

others),” and “a computer user’s Internet activities generally leave traces or ‘footprints’ in the web cache and history files of the browser used.” (Gov’t Ex. 1 at 38–39.) Thus, there was probable cause to search Defendant’s residence because there was a fair probability that they would discover evidence of the completed crime of access with intent to view child pornography. *See Huyck*, 849 F.3d at 440; *see also Tagg*, 886 F.3d at 590 (holding that a warrant may issue “when law enforcement shows that the suspect (a) accessed a website containing actual child pornography, and (b) browsed the site for an extended period of time while clicking on links that were blatant advertisements for child pornography”).

Defendant also argues that the search warrant lacked probable cause because the facts supporting its issuance were stale. (Def.’s Mem. 7–11.) SA Blackmore executed the warrant on July 29, 2015, almost exactly five months after the last documented Website A activity on February 20, 2015. The Eighth Circuit has rejected staleness challenges in child pornography cases with the same or longer lapses of time. *See United States v. Estey*, 595 F.3d 836, 840 (8th Cir. 2010) (“[T]his case involves a search warrant issued five months after discovering information linking the defendant’s residence with child pornography. This Court, and others, have held that evidence developed within several months of an application for a search warrant for a child pornography collection and related evidence is not stale.”). As the court explained in *Huyck*, “‘child pornographers generally retain their pornography for extended periods.’” 849 F.3d at 439–40 (quoting *United States v. Chrobak*, 289 F.3d 1043, 1046 (8th Cir. 2002)).

Defendant argues that the information in the affidavit was stale due to the abrupt shutdown of Website A. (Def.'s Mem. 11.) This, according to Defendant, would have alerted a suspected user (such as Defendant) that the site was being monitored by law enforcement, prompting the user to destroy incriminating evidence. (*See id.*) The possibility that evidence could have been destroyed does not render information in the affidavit stale or undermine the existence of probable cause. As noted above, the affidavit states that digital information is durable and can be saved unintentionally.[6] Therefore, the information in SA Blackmore's affidavit was not stale, and the warrant was supported by probable cause.

B. Good Faith Exception

Evidence obtained pursuant to a search warrant that is later determined to be invalid is excepted from the exclusionary rule "'when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope.'" *United States v. Rodriguez*, 834 F.3d 937, 941 (8th Cir. 2016) (quoting *United States v. Leon*, 468 U.S. 897, 920 (1984)). Courts give "'great deference' to a magistrate's determination" that probable cause existed to issue a warrant. *Leon*, 468 U.S. at 914 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)). "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or

[6] Defendant may have destroyed or discarded the computer he used for his Website A activity because it was not located in his home on the day of the search. The FBI located a backup copy of that computer on another hard drive, containing evidence used to charge Defendant with several counts in this case. (*See* Gov't's Mem. 13 n.3.)

could not have harbored an objectively reasonable belief in the existence of probable cause." *United States v. Cannon*, 703 F.3d 407, 412 (8th Cir. 2013). The following circumstances preclude a finding that officers acted in objective good faith in executing a warrant:

> (1) When the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the issuing judge wholly abandoned his judicial role in issuing the warrant; (3) when the affidavit in support of the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) when the warrant is so facially deficient that no police officer could reasonably presume the warrant to be valid.

United States v. Hopkins, 824 F.3d 726, 733 (8th Cir. 2016).

Defendant argues that no reasonably well-trained agent would believe that SA Blackmore's affidavit contained the requisite probable cause to search Defendant's residence for child pornography. (Def.'s Mem. 13.) Defendant emphasizes that while the affidavit is 44 pages long, Defendant is only alleged to have accessed Website A on four occasions. (*Id.*) This argument mischaracterizes the substance of the affidavit, which plainly states that the four posts described therein are "[e]xamples and descriptions," not the full extent of Defendant's activities. (Gov't Ex. 1 at 27–28.) As noted above, the affidavit explains that "baddaddy" was actively logged into the website for a total of 112 hours and 52 minutes between November 26, 2014, and February 24, 2015. (*Id.* at 26.) Therefore, the warrant was not facially deficient or so lacking in indicia of probable

cause as to render official belief in its existence entirely unreasonable, and the good faith exception to the exclusionary rule is applicable.[7]

RECOMMENDATION

Based on the above files, and the records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Defendant's Motion to Suppress Evidence Obtained From the Search of Defendant's Residence (Doc. No. 22) be **DENIED**.

Date: August 22, 2018.

s/ Becky R. Thorson
BECKY R. THORSON
United States Magistrate Judge

NOTICE

Filing Objections: This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals. Under Local Rule 72.2(b)(1), a party may file and serve specific written objections to this Report within **fourteen days**. A party may respond to those objections within **fourteen days** after service thereof. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set forth in LR 72.2(c).

[7] Defendant cites and discusses a Third Circuit opinion at various points in his brief. *See United States v. Zimmerman*, 277 F.3d 426 (3d Cir. 2002) (reversing denial of motion to suppress search warrant seeking evidence of possession of child and adult pornography). This case is distinguishable for a variety of reasons, including that the Government conceded that there was no probable cause to search the home for child pornography because "the affidavit contained no information that Zimmerman had ever purchased or possessed child pornography." *Id.* at 432. Moreover, the officers were searching only for evidence of possession, not evidence of access with intent to view as in the instant case.